Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 09 décembre 2008
N° CERTA-2008-AVI-586

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de la suite logicielle Microsoft Office

Gestion du document

Référence	CERTA-2008-AVI-586
Titre	Multiples vulnérabilités de la suite logicielle Microsoft Office
Date de la première version	09 décembre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-072 du 09 décembre 2008
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Microsoft Office 2000 Service Pack 3 ;
- Microsoft Office XP Service Pack 3 ;
- Microsoft Office 2003 Service Pack 3 ;
- Microsoft Office Word 2007 ;
- Microsoft Office Word 2007 Service Pack 1;
- Microsoft Office Outlook 2007 ;
- Microsoft Office Outlook 2007 Service Pack 1;
- Microsoft Office Word Viewer 2003 ;
- Microsoft Office Word Viewer Service Pack 3 ;
- Microsoft Office Compatibility Pack pour les formats Word, Excel, et PowerPoint ;
- Microsoft Office Compatibility Pack pour les formats Word, Excel, et PowerPoint Service Pack 1;
- Micorsoft Works 8 ;
- Microsoft Office 2004 pour Mac ;

– Microsoft Office 2008 pour Mac ;
– Open XML File Format Converter pour Mac.

3 Résumé

De multiples vulnérabilités ont été découvertes dans la suite logicielle `Microsoft Office`. Ces vulnérabilités peuvent être exploitées afin d'exécuter du code arbitraire à distance.

4 Description

Huit vulnérabilités ont été découvertes dans la suite `Microsoft Office`. Ces vulnérabilités peuvent être exploitées par l'intermédiaire d'un fichier `Word` ou `RTF` spécialement construit. L'interprétation de ce fichier par `Microsoft Word` ou `Microsoft Outlook` permet d'exécuter du code arbitraire quelque soit la vulnérabilité exploitée parmi les huit.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

– Bulletin de sécurité Microsoft MS08-072 du 09 décembre 2008 :
http://www.microsoft.com/france/technet/security/Bulletin/MS08-072.mspx
http://www.microsoft.com/technet/security/Bulletin/MS08-072.mspx
– Référence CVE CVE-2008-4024 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4024
– Référence CVE CVE-2008-4025 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4025
– Référence CVE CVE-2008-4026 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4026
– Référence CVE CVE-2008-4027 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4027
– Référence CVE CVE-2008-4028 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4028
– Référence CVE CVE-2008-4030 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4030
– Référence CVE CVE-2008-4031 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4031
– Référence CVE CVE-2008-4037 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4037

Gestion détaillée du document

09 décembre 2008 version initiale.